MANUAL DE CARGOS

Dependencia:	Dirección de Gestión	**Área:**	División Seguridad de la Información
Código del Cargo:	3011.10	**Código del Puesto:**	3011
Categoría:	21	**Nombre del Puesto:**	Profesional Procesamiento Electrónico de Datos 2
Nombre del Cargo:	Profesional Seguridad de la Información	**Reporta a:**	Jefe División de Seguridad de la Información
Objetivo del Cargo:	Ejecutar y gestionar labores profesionales en diversos procesos correspondientes a la División de Seguridad de la Información, con el fin de cumplir las metas y objetivos establecidos, a su vez, revisar y atender requerimientos varios que sean asignados por la jefatura y brindar apoyo en lo solicitado. Le puede corresponder cumplir un rol especifico de acuerdo con la necesidad de la División, dentro de los roles establecidos en este perfil de cargo están: Gestión, Monitoreo, Incidentes, Planeamiento y Arquitectura.		

MACRO PROCESO	PROCESO	ACTIVIDAD	FUNCIONES PRINCIPALES
	Funciones generales las cuales se deben cumplir en todos los roles		1. Cumplir con la calidad y tiempos de respuesta establecidos para las funciones correspondientes al cargo.
			2. Colaborar a la jefatura en la ejecución de actividades o proyectos establecidos para el Área, División o Dirección de alcance Institucional.
			3. Tener disponibilidad de traslado para la atención de asuntos inherentes a su puesto de trabajo.
			4. Ejecutar otras funciones propias del Área, División o Dirección.
			5. Gestionar los riesgos, brechas, vulnerabilidades y amenazas de la arquitectura Seguridad de la Información.
			6. Participar en la clasificación y protección de la información, así como la gestión de los riesgos.
			7. Gestionar el Programa de Concientización en Seguridad de la Información para el Conglomerado Financiero.
			8. Participar en el seguimiento, coordinación, atención y respuesta de los eventos e incidentes de Seguridad de la Información.
			9. Realizar estudios, análisis, investigaciones, informes y recomendaciones relacionados con la Seguridad de la Información.
			10. Coordinar y trabajar en conjunto con distintos equipos de trabajo en la implementación de los proyectos, iniciativas y/o actividades establecidas en el Plan de Gestión de Seguridad de la Información.
			11. Gestionar Indicadores de la postura de Seguridad de la Información para el Conglomerado Financiero.
			12. Desarrollar y documentar las acciones necesarias para implementar y atender los requerimientos de entes de supervisión y reguladores tanto internos como externos.
			13. Preparar las respuestas mediante oficios a las dependencias solicitantes.
			14. Gestionar, coordinar y/o participar de las iniciativas y actividades del Plan de Gestión de Seguridad de la información del Conglomerado Financiero.
	Rol de Gestión de Activos y Riesgos		15. Gestionar el seguimiento, mantenimiento y monitoreo del Sistema de Gestión de Seguridad de la Información (SGSI).
			16. Administrar y ejecutar las actividades correspondientes para la gestión de los activos de información, así como para los riesgos de seguridad de la información.
			17. Velar por el cumplimiento de los controles de seguridad de la información en relación con los proveedores del Conglomerado Financiero.
			18. Ejecutar el seguimiento y control de las actividades correspondientes al Plan Gestión de Seguridad de la Información del Conglomerado Financiero.
	Rol de Incidentes y monitoreo		19. Realizar seguimiento y monitoreo de atención de alertas de seguridad relacionados con identidad, accesos, herramientas de seguridad, entre otros.
			20. Gestionar el seguimiento, coordinación, atención y respuesta a los eventos e incidentes de Seguridad de la Información relacionados con el Sistema Gestión de Seguridad de la Información (SGSI).
			21. Gestionar la documentación relacionada con la gestión de incidentes de seguridad de la información del Conglomerado Financiero, así como coordinar las investigaciones internas en relación con incidentes de seguridad de la información.
			22. Coordinar la ejecución de análisis Forense dentro del Conglomerado Financiero.
	Rol de Planeación y Operaciones		23. Realizar el mantenimiento del Plan de Gestión de Seguridad de la Información.
			24. Verificar que la planeación de Seguridad de la Información este alineada con los objetivos estratégicos del Conglomerado y normativa aplicable.
			25. Realizar y coordinar con las Dependencias correspondientes la definición de los estándares de líneas base de seguridad de la información relacionados con las herramientas de seguridad.
			26. Ejecutar seguimientos sobre las operaciones de seguridad en cuanto a las herramientas de prevención y detección de amenazas de ciberseguridad.
	Rol de Arquitectura y Seguridad		27. Gestionar los modelos de arquitectura de seguridad alineados con el Sistema de Gestión de Seguridad de la Información (SGSI).
			28. Mantener actualizados los esquemas de arquitectura en coordinación con las dependencias competentes según corresponda (sistemas, seguridad física, seguridad lógica, entre otros).
			29. Gestionar la arquitectura de seguridad del Sistema de Gestión de Seguridad de la Información (SGSI) alineándolo con el cumplimiento de los controles de seguridad de la información.
			30. Definir la arquitectura de seguridad para los proyectos, procesos y herramientas del Conglomerado Financiero.
	Rol de Gobierno y Cumplimiento		31. Atender los distintos entes de supervisión y reguladores tanto internos como externos.
			32. Gestionar el cumplimiento de marcos normativos, leyes y regulaciones relacionadas con: Norma PCI DSS, Acuerdo SUGEF 14-17, CGR, Ley 8968, entre otros.
			33. Participar en foros y comités de gobiernos corporativo que sean requeridos.
			34. Mantener bajo la normativa de seguridad de la información del Conglomerado Financiero, así como evaluar su cumplimiento.
			35. Representar por delegación a la jefatura en reuniones donde se analizan y resuelven asuntos relacionados con la División de Seguridad de la Información.
			36. Autorizar por delegación de la jefatura todos aquellos documentos que lo requieran.
			37. Revisar y analizar documentación en relación con entregables de la División.
			38. Colaborar en la planeación, organización, ejecución y control de las actividades internas de la División.

			FUNCIONES RELACIONADAS CON RIESGO
			39. Realizar una adecuada gestión de los riesgos, identificando, valorando y controlando aquellos que puedan impactar los Planes Estratégicos del Conglomerado a los cuales se encuentran asociados.
			40. Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, relacionados directamente a la administración de los riesgos operativos, normativos, financieros, de proyectos, tecnológicos y reputacionales, según corresponda.
			41. Ejecutar los lineamientos establecidos en la metodología institucional de administración de riesgos del Conglomerado Financiero, así como las herramientas y técnicas para identificar los distintos tipos de riesgos a que se encuentra expuesta la entidad.
			42. Desarrollar las actividades relacionadas con la atención de los Planes de Mitigación de los riesgos identificados dentro de los procesos de la dependencia asignada.
			43. Dar seguimiento al control y fiscalización a las medidas adoptas para el funcionamiento del sistema de valoración del riesgo, garantizando una adecuada cultura de riesgo.
			44. Asegurar que el personal a su cargo conozca sobre la normativa de riesgo aplicable a su área, como parte de la Cultura de Riesgo.
			45. Le puede corresponder participar activamente en los diferentes Comités o comisiones definidos para el Conglomerado para conocer los planes de acción y medidas a tomar para minimizar el impacto de los riesgos inherentes en su campo de acción.
			46. En caso de materializarse un evento de riesgo es responsable de reportarlo directamente a la Dirección Corporativa de Riesgo, para su análisis y seguimiento.
CÓDIGO	**REQUISITOS EXIGIBLES**		
	Formación Académica:	Licenciatura en Ingeniería de Sistemas, en Ingeniería Informática, en Ingeniería de Sistemas Informáticos. Licenciatura en Ingeniería Industrial o Administración de Empresas.	
	Legales:	Incorporado al Colegio Profesional respectivo y estar al día con sus obligaciones.	
	Experiencia:	Tres años de experiencia en gestiones, actividades y proyectos con relación a la seguridad de información en entidades bancarias.	
CÓDIGO	*** REQUISITOS TÉCNICOS EXIGIBLES**		
	1. Certificación normativa ISO/IEC 27001 (Implementador o auditor) o Certificación Gerente de Seguridad de la Información (CISM).		
	2. Conocimiento en fundamentos de Ciberseguridad.		
	3. Conocimiento en los apartados y ámbito de aplicación de la norma de Gestión del Riesgo (ISO 27005).		
*** Los requisitos técnicos exigibles deben ser presentados con respaldo por medio de certificaciones de participación, aprovechamiento, cursos o similares o por medio de la prueba de conocimiento que forma parte del proceso de selección.**			
CÓDIGO	**REQUISITOS TÉCNICOS DESEABLES**		
	1. Conocimiento en la Normativa externa relacionada con la Superintendencia General de Entidades Financieras (SUGEF).		
	2. Conocimiento en la Normativa externa relacionada con la Superintendencia General de Valores (SUGEVAL).		
	3. Conocimiento en la Normativa externa relacionada con la Superintendencia de Pensiones (SUPEN).		
	4. Conocimiento en la Normativa externa relacionada con la Contraloría General de la República.		
	5. Conocimiento en la Normativa externa relacionada con el Banco Central.		
	6. Conocimiento en el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF).		
	7. Conocimiento en la Normativa externa relacionada con el Cumplimiento de la Ley 8204.		
	8. Conocimiento en la Normativa Interna del Conglomerado Financiero.		
	9. Conocimiento en Hacker Ético Básico.		
	10. Conocimiento avanzado en las Mejores prácticas en TI (COBIT, ITIL o ISO 27000).		
	11. Conocimiento en Autorías de Sistemas Básico.		
	12. Conocimiento en la Planificación y Administración del Tiempo.		
	13. Conocimiento en procesos de Investigación.		
	14. Conocimiento en la ejecución de Informes Profesionales.		
	15. Conocimiento en Análisis Forenses.		
	16. Conocimiento básico en Autorías de Sistemas.		
	17. Certificaciones Avanzadas en CISA y/o CRISC.		
CÓDIGO	**SISTEMAS UTILIZADOS**		
	Sistema de Gestión de Seguridad de la Información (SGSI).		
	Herramientas de seguridad informática a modo de supervisión (lectura).		
	Word, Excel, Power Point, Outlook.		

	COMPETENCIAS REQUERIDAS				
PERFIL KOMPE DISC:		PERFIL: PROFESIONALES SOPORTE			
CÓDIGO	**Cardinales:**	**D**	**C**	**B**	**A**
CAR-01	Compromiso Social				
CAR-02	Orientación al Cliente				
CAR-03	Innovación y Creatividad				
CAR-04	Orientación al Logro				
CAR-05	Seguimiento de procedimientos				
CÓDIGO	**Gerenciales:**	**D**	**C**	**B**	**A**
GER-01	Desarrollo de Otros				
GER-02	Dirección de Equipo				
GER-03	Seguimiento de la Gestión				
CÓDIGO	**Del Negocio:**	**D**	**C**	**B**	**A**
NEG-01	Análisis de la Información				
NEG-02	Negociación				
NEG-03	Persuasión				
NEG-04	Manejo Emocional				
NEG-05	Trabajo en Equipo				
CÓDIGO	**Del Soporte:**	**D**	**C**	**B**	**A**
SOP-01	Planeación				
SOP-02	Practicidad				
SOP-03	Precisión				
CÓDIGO	**DISC - Personalidad**	**D**	**C**	**B**	**A**
DISC-01	Dominancia				
DISC-02	Influencia				
DISC-03	Estabilidad				
DISC-04	Conformidad				
Observaciones:	**Se crea perfil de cargo, unificando los perfiles de cargo existentes (Profesional Seguridad de la Información-Monitoreo, Profesional Seguridad de la Información-Incidentes y Profesional Seguridad de la Información-Planeamiento) mediante la aprobación de la Gerencia General Corporativa en el HT-558-GGC-2019, de fecha 18 de noviembre de 2019.** **Se agregan las funciones Relacionadas con Riesgo, según autorización brindada por la Gerencia General Corporativa mediante HT-493-GGC-2019, de fecha 14 de octubre de 2019.**				